security 101
技術編

Identity Management とProvisioning の重要性

～ 国防総省は、なぜセキュアOSを作らせたのか ～

佐藤　慶浩
日本ヒューレット・パッカード株式会社

IPA セキュリティセンター 非常勤研究員

2002 年 10月 4日

Slide 1

security 101
技術編

Trusted OS モデルの一覧

TCSEC BLS (B level security) / US DoD
CMWEC (Compartmented Mode Workstation) / TAC4 for US NAVY
Post Bell-La Padula model

ご紹介するセキュリティ用語

Identity Management
Provisioning

Slide 2

Trusted OS の活用

講師略歴

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード株式会社
ＨＰコンサルティング事業統括本部
セキュリティ・コンサルティング部　部長

1986 年。日本アポロコンピュータ(株)入社。International R&Dに所属。マサチューセッツ州チェルムスフォード市にて日本語環境製品の開発に従事。
1990 年。日本ヒューレット・パッカード(株)入社。新製品のテクニカル・マーケティングとして、ＯＳＦ／1、分散環境コンピューティング技術、マルチメディア技術、ハイアベイラビリティ技術、インターネット技術をＨＰ社の製品提供と相応して順次担当。この間 1993 年からの 2 年間はカリフォルニア州クパチノ市にてセキュリティ製品の仕様開発に従事。
1996 年、米国駐在中に計画した製品群の出荷が始まったため、現在は主としてセキュリティ・ソリューションのコンサルティングに従事している。
1997 年以後は、通常のコンサルティング活動の他に、ＪＰＣＥＲＴ／ＣＣのヒューレット・パッカード対応窓口を担当。また、ＦＩＳＣ(金融情報システムセンタ)、ＪＩＳＡ（情報サービス産業協会）、ＪＵＡＳ（日本情報システム・ユーザ協会）、システム監査人協会や各種有料セミナにて情報セキュリティポリシー策定方法論についての講演をしている。

情報処理学会(www.ipsj.or.jp/)　正会員
日本ネットワークセキュリティ協会(www.jnsa.org/)　理事
情報処理振興事業協会(www.ipa.go.jp/)セキュリティセンター　非常勤研究員
金融情報サービスセンター(www.fisc.or.jp/)セキュリティポリシー研究会　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) SC 27/WG 1 小委員会　委員
杉並区住基ネット調査会(www.city.suginami.tokyo.jp/)　技術専門委員
情報ネットワーク法学会(www.in-law.jp/) 理事

Trusted OS の活用

バッファー・オーバー・ラン問題への対策

予防：
アプリケーション開発のガイドライン遵守

http://www.ipa.go.jp/security/awareness/vendor/programming/intro.html

保護：
最新のパッチの適用
アプリケーションレベルのセキュリティ製品の導入
カーネルレベルのＯＳセキュリティ強化

検出：
侵害検出システムの導入
　ネットワークベース、ホストベース、ファイルベース、カーネルベース

対応：
インシデント対応体制と手順の確立

Trusted OS の活用

まずは、結論から

- ◆DMZの復習 1
- ◆まずは解決策を先に 2
- ◆TCSEC-BLS, CMWEC 3

Slide 5

Trusted OS の活用

OSのセキュリティ強度が問われている

- ◆OpenHack 2 (Y2000)
  ファイアウォール（＋IDS）＋サーバ
- ◆OpenHack 3 (Y2001)
  サーバのみ

ファイアウォールベンダが採用するサーバOS

Slide 6

Trusted OS の活用

BLS は何がしたかったのか？
→ 5A の確立

Authentication	真正確認
Access Control	アクセス制御
Authorization	アクセス権管理
Auditing	監査
Assurance	保証

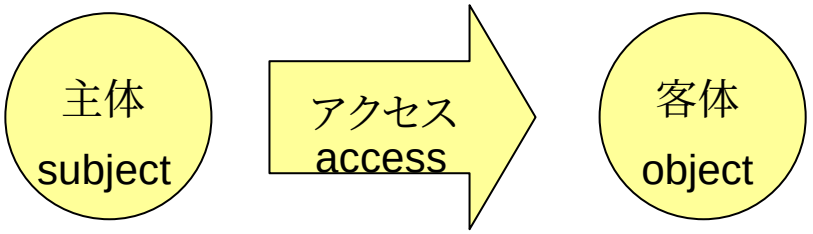
User authentication	本人確認
Terminal authentication	端末確認
Server authentication	サーバ確認

Slide 7

Trusted OS の活用

情報セキュリティ対策とは？

主体が客体にアクセスする上での
機密性、完全性、可用性を守ること



Slide 8

Trusted OS の活用

誰に何を許可するのか

不正アクセス　illegal access

無許可アクセス　unauthorized access
許可の濫用　abuse of authorized access

無許可アクセス：
- ◆結果検出
- ◆起こってはならないはずのこと
- ◆技術的保護違反

許可の濫用
- ◆行使検出
- ◆ (やればできるけど)やってはならないこと
- ◆運用規定違反

→ ◆変則検出 (anomaly detection)

Slide 9

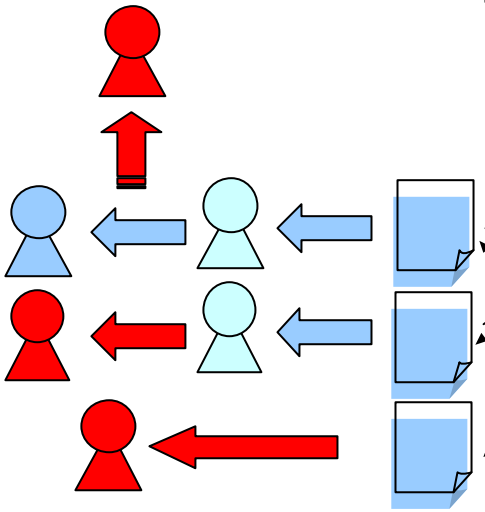
Trusted OS の活用

主体の責務

◆CIA のうち C の例

漏洩

主体の意図
- ある　→保護、検出
- ない
  - 過失
    - ― 誤送　→予防
  - 不可避
    - ― 盗聴　→保護
    - ― 詐取　→予防



Slide 10

Trusted OS の活用

客体の格付け

CLASSIFICATION

DESIGN CLASSIFICATION MODEL
- clearances
- sensitivity levels + compartments
- markings - (worst practice: floating label)

HOW TO BE HANDLED (not based on attribute)

CRITERIA TO CLASSIFY
- when? at creation (concern about 1:N)
- who? by creator (concern about 1:N)
- what? Just Enough (is better than Baseline)

Slide 11

Trusted OS の活用

客体の格付け

Step 1.4 ポリシー群の洗い出し

重要度の明確化
情報種別
システム種別

格付け（Classification）＝重要度の格と表現方法の**定義**

表記義務の明文化

機密性 例：極秘、関係者外秘、秘、非機密）
完全性 例：最重要、重要、一般）
可用性 例：最重要、重要、一般）

×

情報
情報システム

度合い 例：上記） ｜ 種別 例：人事秘、顧客情報）
マーキング 例：禁帯出、禁複製）

(Level, Compartment & Marking)

Slide 12

Trusted OS の活用

情報セキュリティポリシーの必要性

◆情報セキュリティポリシーで「人の役割」と「情報の格付け」が重要とされる所以

security strength
depends on audit
enforced by integrity
ex) WRITE UP
makes containment
against abuse of authorization

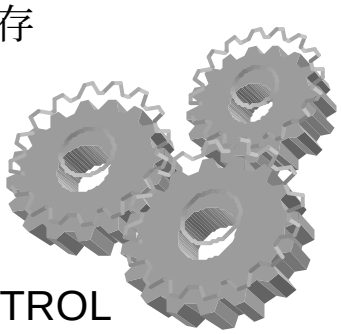
性善説を前提
性悪説を想定
~~内部/外部~~

◆強固な監査機構の装備による抑止効果

Slide 13

Trusted OS の活用

基礎技術要素の相互依存



CLASSIFICATION
AUTHENTICATION
ACCESS CONTROL
INFORMATION FLOW CONTROL
LEAST PRIVILEGE
AUTHORIZATION (DUAL LOCK)
AUDITING

◆システムのセキュリティ強度は、そのシステムの監査証跡（Audit Trail）の保全性強度に依る

covert channel

Slide 14

Trusted OS の活用

DUAL LOCKED AUTHORIZATION

sysadmin	本人	i.s. system officer
	(sysadmin に申請)	
①アカウント作成 ②パスワード初期化 (本人に通知)	③パスワード設定 (isso に報告)	④アクセス権限付与 ⑤アカウント活性化

管理者は管理権限以外のアクセス権を得られないようにすべきである。

◆司法取引（免罪制度）の前提

利用者(user) 所有者(owner)
保管者(custodian) 保護者(guardian)

Trusted OS の活用

情報セキュリティ啓発と教育

情報の取り扱い

情報の格付け
表記義務 ― 格付けを表記しなければ伝わらない
注意義務 ― 格付けに従った取り扱いの徹底
報告義務 ― 格付けの設定・取り扱い誤りの報告

◆発見時点では、違反ではなく「誤り」としての対応
◆「始末書」ではなく、「理由書」

Trusted OS の活用

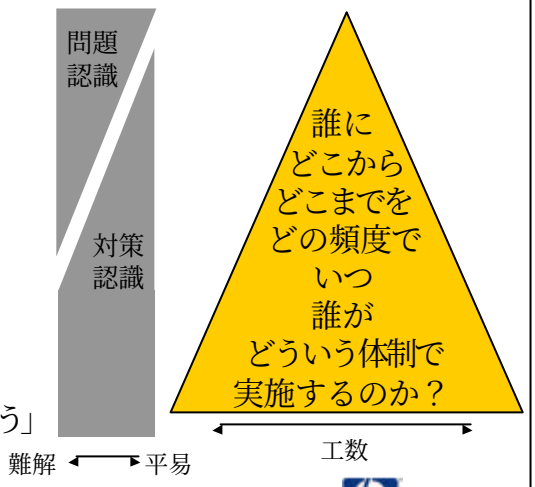
情報セキュリティ啓発と教育

周知・徹底の 3 つのレベル

Step 4.1 啓発（awareness）
知識
「知ってもらう」

Step 4.2 教育（education）
理解
「正しくわかってもらう」

Step 4.3 訓練（training）
実践
「できるようになってもらう」



Slide 17

Trusted OS の活用

それでも破られる。に違いない。

	事前 proactive	事後 reactive
予防 PREVENTION	X	
保護 PROTECTION	X	
検査 penetration	x	
検出 detection	x	
対応 REACTION		X
報告 REPORT		X

plan in advance

incident

improve

* trap (pitfall on the term “REACTION”)

Slide 18

Trusted OS の活用

製品評価

ISO/IEC 15408 (JIS X5070)

TOE - Target of Evaluation - 企画書
PP - Protection Profile - 要件定義書
ST - Security Target - 設計仕様書
EAL - Evaluation Assurance Level

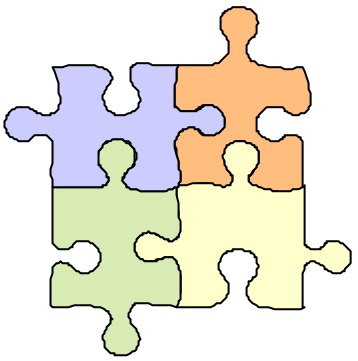
注意！
EAL はセキュリティ強度と無関係

Trusted OS の活用

国際動向とアメリカ動向

ISO/IEC 15408　　JIS X 5070
CC V2.1

CCRA



Common Criteria

Partnership with ISO

- Common Criteria development group made significant effort to get criteria adopted as an international standard (ISO/IEC 15408)
- Need to maintain regular and consistent coordination/liaison with ISO SC 27 Working Group 3—but this effort requires resources which tend to be limited

出典: 以下の講演資料から抜粋
CCRA History, Implementation, Future E`xpansion, and International Experiences
Dr. Stuart Katzke / National Institute of Standards and Technology

Common Criteria

•No new versions until April 2003 (at the earliest)

Request for Interpretations (as of February 2002)

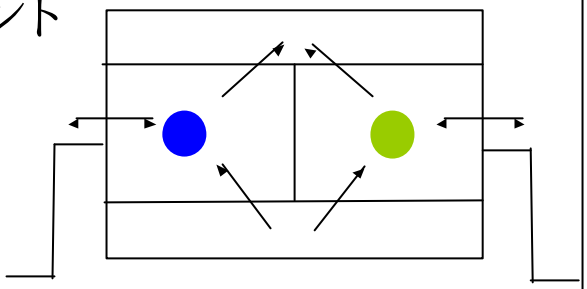
- 206 Total Requests for Interpretation
- Final interpretation is a change to the CC/CEM
- 16 months average time to process
  - Labor intensive: requires significant preparation/coordination
  - Limited resources
  - Requires unanimous consent

出典: 以下の講演資料から抜粋
Future Directions of the Common Criteria (CC) and the Common Evaluation Methodology (CEM)
Dr. Stuart Katzke / National Institute of Standards and Technology

Trusted OS の活用

Bell-La Padula モデル 商用を阻害する要因

ラベル
フローコントロール
コンパートメント



Slide 23

Trusted OS の活用

Bell-La Padula モデルの後継

hp secure linux の例

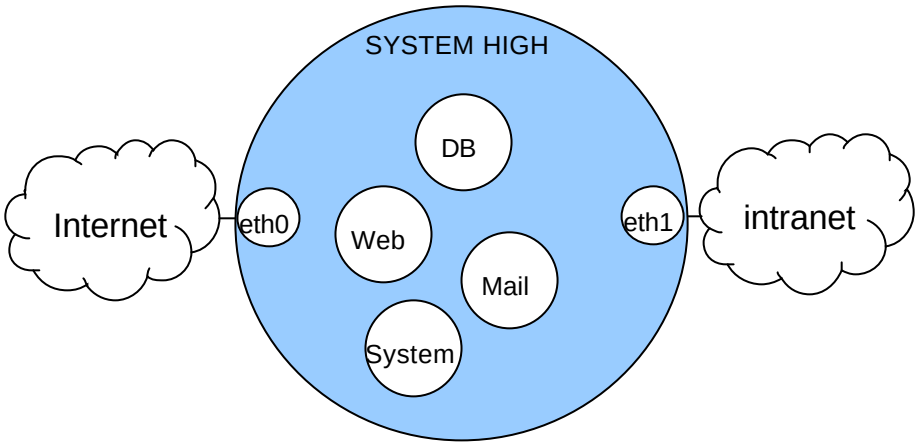
その他の例

参考資料

Slide 24

Trusted OS の活用

コミュニケーション制御



Slide 25

Trusted OS の活用

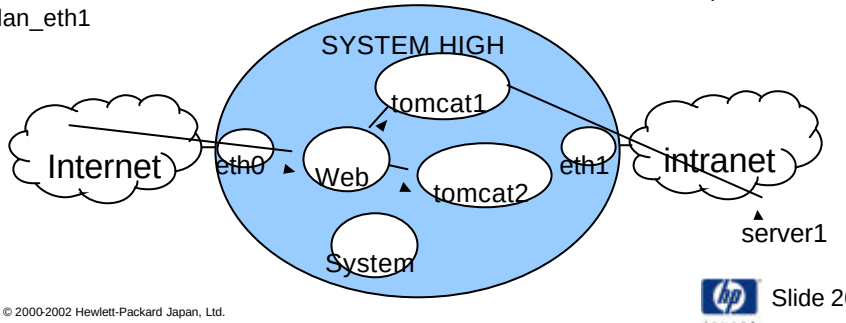
コミュニケーション制御

HOST * -> COMPARTMENT web PORT 80 METHOD tcp NETDEV lan_eth0

COMPARTMENT web -> COMPARTMENT tomcat1 PORT 8007 METHOD tcp NETDEV lan_lo

COMPARTMENT web -> COMPARTMENT tomcat2 PORT 8008 METHOD tcp NETDEV lan_lo

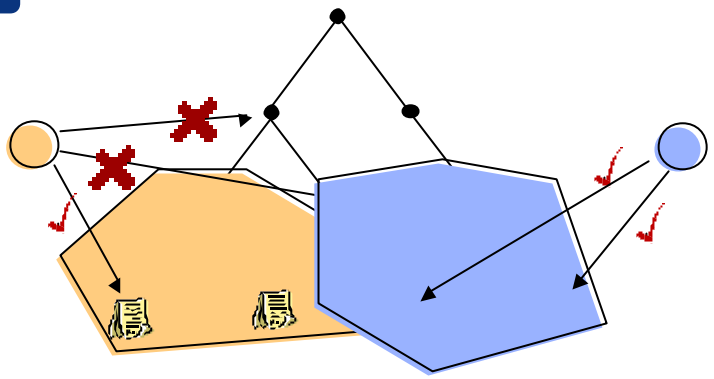
COMPARTMENT tomcat1 -> HOST server1 PORT 8080 METHOD tcp NETDEV lan_eth1



Slide 26

Trusted OS の活用

ファイルシステム制御

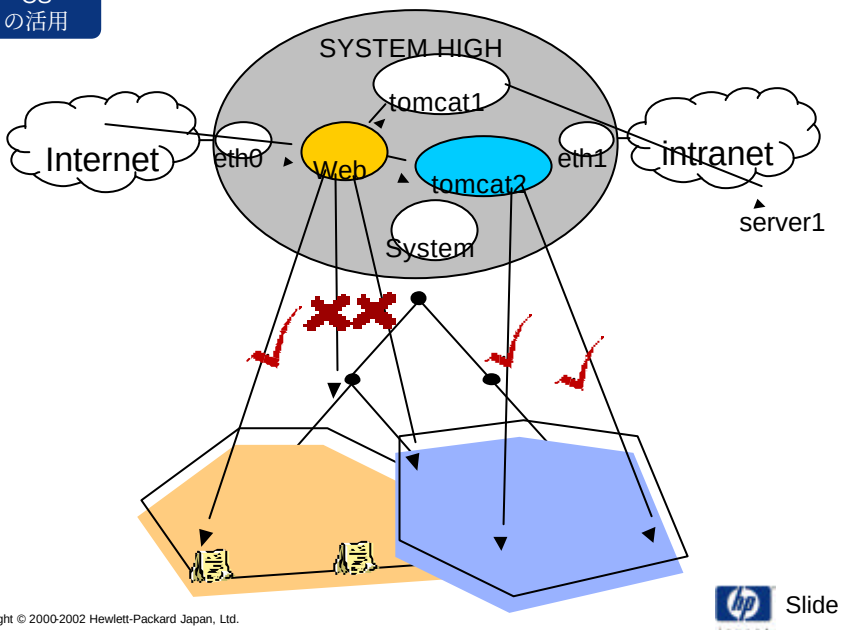


```
web /compt/web read active
web /compt/web/tmp read,write active
web /compt/web/apache/logs append active
web / none active
```


Slide 27

Trusted OS の活用

コミュニケーション制御とファイルシステム制御



Slide 28

Trusted OS の活用

hp secure linux 実機デモ

```
# ls -ln
-rw-r--r-- 1 0 0   348 Nov 16 04:45 access.conf
-rw-r--r-- 1 0 0 43796 Nov 16 04:45 httpd.conf
-rw-r--r-- 1 0 0 11317 Nov 16 04:45 mime.types
-rw-r--r-- 1 0 0   357 Nov 16 04:45 srm.conf
-rwxrwxrwx 1 0 0    46 Dec 24 23:32 openfile
# echo abc > httpd.conf
sh: httpd.conf: Operation not permitted
# who
root tty1  Dec 25 03:10
# echo abc >> openfile
sh: openfile: Operation not permitted
# rm access.conf
rm: cannot unlink ‘access.conf’: Operation not
#
```

Trusted OS の活用

Bell-La Padula モデルの後継

hp secure linux の例

その他の例 ppt

参考資料 PDF

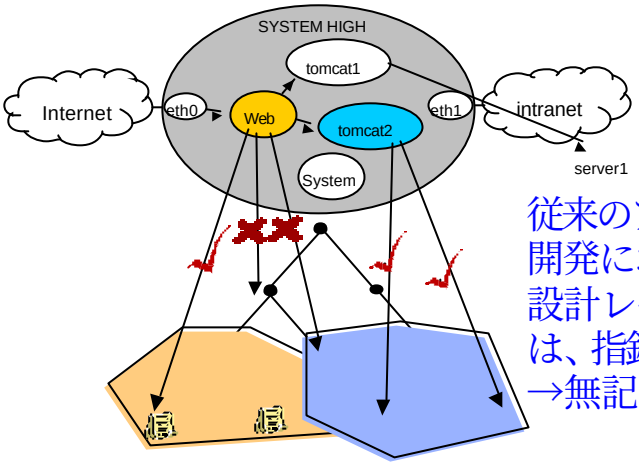
http://www.ipa.go.jp/security/fy13/report/secure_os/secure_os.html

Slide 30

Trusted OS の活用

Bell-La Padula モデルの後継の利点

論理設計書でのセキュリティ要件記述の実効性



従来のアプリケーション開発においては、論理設計レベルの要件記述は、指針でしかなかった。
→無記述の要因のひとつ

Slide 31

Trusted OS の活用

Bell-La Padula モデルの用途

ラベル方式　（Bell-La Padula モデル）
- 利用者がシステムに直接ログオンして利用する
- クライアントマシン
- セキュリティ厳格
- アプリケーションのＢＬS対応開発必要
- 中核サーバには必須

非ラベル方式
- ネットワークを経由してサービスを利用する
- サーバマシン
- 市販アプリの利用を促進

Slide 32

Trusted OS の活用

BLS は何がしたかったのか？
→ 5A の確立

Authentication	真正確認	Authentication
Access Control	アクセス制御	Authorization
Authorization	アクセス権管理	Administration
Auditing	監査	
Assurance	保証	

User authentication	本人確認
Terminal/Client/Device authentication	端末確認
Server authentication	サーバ確認

Slide 33

Trusted OS の活用

対処療法 と 恒常的対策

ファイアウォールだけで守る。
→不毛

最新のパッチを即座に適用する。
→対処療法 →少なくない運用経費

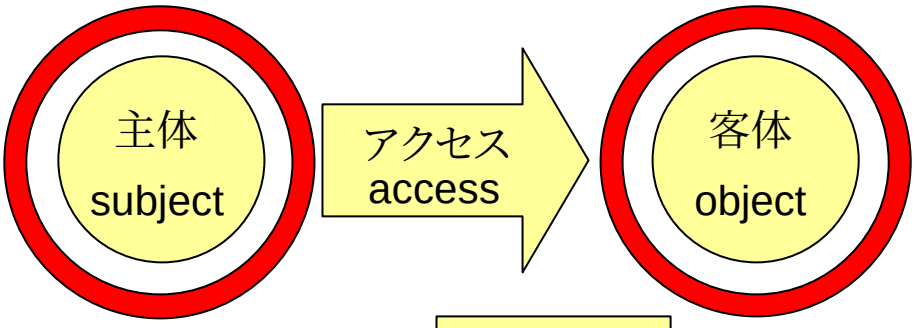
制御を奪取されないようにする。
→完全回避不可能

Slide 34

Trusted OS の活用

情報セキュリティ対策とは？

主体が客体にアクセスする上での
機密性、完全性、可用性を守ること



- クラサバ等のC→Sの連鎖
- Web利用者とWebコンテンツ
- Web利用者とキーボード

Trusted OS の活用

Trusted OS の効能

未知の攻撃手法への対策

最新パッチの適用の時間的猶予を得る
→大幅な運用経費軽減

侵害によって発生する被害の最小化を得る
→リスクの低減

原則： 受け入れリスクの許容)
侵入されてもC IAを侵害されなければよい

A の侵害は防げない。

Trusted OS の活用

軍用 Military grade への期待範囲

C
I
A
} Military

	主体の意思	
	◆ある	◆ない
C	対象	想定していない
I	対象	(A)
A	✘	対象

Slide 37

Trusted OS の活用

ご紹介したセキュリティ用語

Identity Management

情報へのアクセスについて、「人」を特定する精度を高めなければならない。
管理の対象は、IDではなく、「人」の特定を目標にすべきである。

Provisioning

情報へのアクセスの最高権限を、システム管理者でさえも、不正行使できないような運用をしなければならない。
最重要な情報保護は、技術だけではなく、運用を通じて暗黙の例外なく、担保することを目標にすべきである。

Slide 38

Trusted OS の活用

Word from MORPHEUS

扉は自分で開け
道を知ることと　歩くことは違う

http:// yosihiro.com /

してあげられることは、道を教えることまで。
あるくのは、自分なのだから。

Slide 40